NOTE ON THE POSSIBLE NUMBER OF OPERATORS OF ORDER 2 IN A GROUP OF ORDER 2^m

By G. A. Miller

It is well known that there is only one group of order 2^m in which all the operators besides the identity are of order 2; viz. the abelian group of type $(1, 1, 1, \cdots)$. In every other abelian group the number of the operators of order 2 is less than half the order of the group. There are, however, many different types of non-abelian groups in which the number of operators of order 2 is more than half the order of the group. The present paper is devoted to the non-abelian groups of order 2^m which have this property. The main object is to prove that the number of operators whose orders exceed 2 can always be obtained by multiplying the order of the group by one of the following infinite system of fractions:

$$\frac{1}{4}, \frac{3}{8}, \frac{7}{16}, \frac{15}{32}, \cdots, \frac{2^n-1}{2^{n+1}}, \cdots.$$

Let G be any non-abelian group in which more than half the operators are of order 2, and let H represent the subgroup of G which is composed of all the operators of G which are commutative with a non-invariant operator (t) of order 2 contained in G.* Since t is not commutative with any operator of $G-H$, it follows that $G-H$ cannot contain more operators of order 2 than of higher orders; for the product of t into any such operator of order 2 is of an order which exceeds 2. Since $G-H$ must include at least one-half of the operators of G, it results that at least one-fourth of the operators of G must have orders which exceed 2. Moreover, there is a group of order 8 (the octic group) in which there are five operators of order 2 and two operators of order 4. Hence there are many groups in which this lower limit is attained; viz. the direct products of the octic group and abelian groups of order 2^α and of type $(1, 1, 1, \cdots)$. In what follows it will be assumed that G is of order 2^m.

---

* Such a non-invariant operator must exist in G since G is generated by its operators of order 2.

1. General properties of G. Let t and H be defined as in the preceding paragraph. If H is abelian it must be of type $(1, 1, 1, \cdots)$ since more than half of its operators are of order 2. If H is non-abelian it must contain a non-invariant operator (t_1) of order 2. All the operators of H which are commutative with t_1 constitute a subgroup (H_1) such that $H - H_1$ contains at least as many operators whose orders exceed 2 as there are of order 2. By continuing this process we finally arrive at an abelian subgroup of type $(1, 1, 1, \cdots)$. Moreover, the quotient group corresponding to the commutator subgroup of G is also of this type, since more than half the operators of G are of order 2.

From the form of the commutator quotient group it follows that the commutator subgroup includes the square of every operator in G. It is also easy to see directly that the square of every operator of G is a commutator, since any operator whose order exceeds 2 multiplied into some operator of order 2 must give a product of order 2; i. e. every operator of G is transformed into its inverse by some operators of order 2 contained in G.*

It will be convenient to employ a quotient group whose order is twice the order of the commutator quotient group; viz. the quotient group (I) which corresponds to an invariant subgroup of G which is composed of half its commutator subgroup. From the fact that the commutator quotient group is the largest possible abelian quotient group, it follows that I is non-abelian. It results from the given isomorphism that the commutator subgroup of I is of order 2, and that the operator of order 2 in this commutator subgroup is the square of every operator of order 4 contained in I. Moreover, over half the operators of I are of order 2 since G has this property. As I is of fundamental importance in what follows we proceed to determine some of its other properties.

2. The quotient group I. Since the commutator subgroup of I is cyclic its group of cogredient isomorphisms is of order 2^{2n}.† Let t_1 be any non-invariant operator of order 2 contained in I. The subgroup (I_1) of I which is composed of all the operators of I which are commutative with t_1 is of order 2^{l-1}, 2^l being the order of I. It is clear that the order of the group of cogredient isomorphisms of I_1 cannot exceed $2^{2(n-1)}$, since I_1 contains more invariant operators than I does and is of a lower order than I. It will soon

* This result is true for every possible group in which more than half the operators are of order 2.

† Fite, *Transactions of the American Mathematical Society*, vol. 3 (1902), p. 342.

appear that this group of cogredient isomorphisms is exactly of order $2^{2(n-1)}$. Just half the operators of $I - I_1$ are of order 2, the remaining operators being of order 4. This follows directly from the fact that the product of t_1 into any operator of order 2 in $I - I_1$ is of order 4, while the product of t_1 into any operator of order 4 in $I - I_1$ is of order 2.

If I_1 is abelian it is of type $(1, 1, 1, \cdots)$, since it is generated by its operators of order 2. If it is not abelian it contains a non-invariant operator (t_2) of order 2. The subgroup of I_1 which is composed of all its operators which are commutative with t_2 is of order 2^{l-2} and the order of its group of cogredient isomorphisms cannot exceed $2^{2(n-2)}$. Continuing this process we arrive at an abelian subgroup of type $(1, 1, 1, \cdots)$ which includes t_1. This subgroup is invariant since it includes the commutator subgroup of I.* Its order is at least 2^{l-n}.

The order of this abelian subgroup of I cannot exceed 2^{l-n} as may be readily seen by reversing the operations of the preceding paragraph. That is, at least half of its operators are invariant in any subgroup of I of double its order in which it may be included. At least one-fourth of its operators are invariant in the subgroup of double the order of the last subgroup and including this subgroup, etc. Hence we have the important theorem: *Every non-invariant operator of order* 2 *contained in I is contained in an abelian subgroup of order 2^{l-n} and of type* $(1, 1, 1, \cdots)$ *but in no larger abelian subgroup of I.*

All the invariant operators of I (besides the identity) are of order 2 and generate a subgroup of order 2^{l-2n}. Hence the non-invariant operators of order 2 may be united into distinct sets of $(2^n - 1)2^{l-2n}$ such that all the operators of a set are commutative. It follows from the fact that just half the operators of $I - I_1$ are of order 2, that the number of operators whose orders exceed 2 in I is

$$\left(\frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^{n+1}}\right)2^l = \frac{2^n - 1}{2^{n+1}}\, 2^l.$$

This proves that *there are groups in which the number of operators whose orders exceed* 2 *is obtained by multiplying the order of the group by* $\frac{2^n - 1}{2^{n+1}}$, *n being any positive integer.*

* *Bulletin of the American Mathematical Society*, vol. 11 (1905), p. 367.

3. Number of operators whose orders exceed 2 contained in G. The only conditions which G is supposed to satisfy are that its order is 2^m and that more than half its operators are of order 2. The object is to prove that the number of operators whose orders exceed 2 contained in G can always be obtained by multiplying its order by a fraction which is of the form

$$\frac{2^a - 1}{2^{a+1}}.$$

For instance, if more than one-fourth of the operators of G have orders which exceed 2, then it follows that at least three-eighths of its operators have this property; if more than three-eighths have this property, it follows that at least seven-sixteenths have the same property; etc.

From the preceding section it follows that the theorem in question requires no proof if all the operators of G which correspond to the identity or to operators of order 2 in I are either the identity or of order 2 Let H be the subgroup of G which corresponds to I_1 in I. Since the order of H is less than the order of G and since H satisfies the conditions which G is supposed to satisfy we shall assume that the theorem in question is true with respect to H; that is, the number of operators in H whose orders exceed 2 is

$$\frac{2^a - 1}{2^{a+1}} h,$$

h being the order of H. From the preceding section it follows that $a > n - 2$, since the group of cogredient isomorphisms of I_1 is of order $2^{2(n-1)}$ and the relative number of operators whose orders exceed 2 must be at least as large in H as in I_1.

The theorem in question is easily seen to be true whenever all the operators of G which correspond to operators of order 2 in $I - I_1$ are also of order 2; for

$$\frac{2^a - 1}{2^{a+1}} h = \frac{2^a - 1}{2^{a+2}} g,$$

g being the order of G, and

$$\frac{2^a - 1}{2^{a+2}} g + \frac{g}{4} = \frac{2^{a+1} - 1}{2^{a+2}} g,$$

which is of the required form. Moreover, if there is one operator whose order exceeds 2 in G among those which correspond to operators of order 2

in $I - I_1$, the number of the operators of G which have this property cannot be less than 2^{m-n-3}. This important theorem may be proved as follows: The corresponding operator in $I - I_1$ is contained in an abelian group of type $(1, 1, 1, \cdots)$ and of order 2^{l-n}. To this abelian subgroup there corresponds in G a subgroup of order 2^{m-n}. The number of the operators of this subgroup which correspond to operators of order 2 in $I - I_1$ is 2^{m-n-1}. At least one-fourth of these are of orders which exceed 2;* i. e. the number of these operators is at least 2^{m-n-3}.

It is now easy to see that $a < n + 1$ whenever operators whose orders exceed 2 correspond to operators of order 2 in $I - I_1$. In fact, if $a = n + 1$ the number of operators whose orders exceed 2 in H would be

$$\frac{2^{n+1} - 1}{2^{n+3}}\, g,$$

and the total number of such operators in G would be at least

$$\left(\frac{2^{n+1} - 1}{2^{n+3}} + \frac{1}{2^{n+3}} + \frac{1}{4}\right) g = \frac{g}{2},$$

which is contrary to the hypothesis that more than half the operators of G are of order 2. It remains therefore only to consider the cases when $a = n - 1$ or n.

When $a = n - 1$, all the operators whose orders exceed 2 in H correspond to operators of order 4 in I_1. If any operators whose orders exceed 2 correspond to operators of order 2 in $I - I_1$ we may use a different H such that a is not less than n. Hence the only case which requires further consideration is when $a = n$ and when there are also operators whose orders exceed 2 corresponding to operators of order 2 in $I - I_1$. Let K represent the abelian subgroup of order 2^{l-n} which contains such an operator of order 2 in $I - I_1$, and let the corresponding subgroup of G be K'.

If the part of K' which corresponds to operators of I_1 contained no operators of order 2, at least 2^{m-n-2} of the operators of G would correspond to operators of order 2 in $I - I_1$. This is impossible since

$$\left(\frac{2^{n} - 1}{2^{n+2}} + \frac{1}{2^{n+2}} + \frac{1}{4}\right) g = \frac{g}{2}\,.$$

* This follows from the theorem that an operator must transform every operator of a group into its inverse if it transforms more than three-fourths of its operators into their inverses.

Moreover, not more than one-fourth of the operators of K' which correspond to operators of I_1 can be of orders larger than 2, since the number of operators of H which have this property is only

$$\frac{2^n-1}{2^{n+1}}\,h.$$

Not more than one-fourth of the operators of K' could be of orders which exceed 2, for if three-eighths of its operators had this property it would again follow that half the operators of G would have the same property.

As just one-fourth of the operators of K' which correspond to operators of order 2 in $I - I_1$ are of orders which exceed 2, the number of operators in G which have this property is

$$\left(\frac{2^n-1}{2^{n+2}}+\frac{1}{2^{n+3}}+\frac{1}{4}\right)g=\frac{2^{n+2}-1}{2^{n+3}}\,g.$$

This completes the proof of the theorem in question and furnishes a fundamental theorem relating to groups of order 2^m.

STANFORD UNIVERSITY.